A FORMAL APPROACH "À LA NEUKIRCH" OF ℓ-ADIC CLASS FIELD THEORY

Stéphanie Reglade

Abstract: *On the one hand Neurkirch has developed general class field theory in his book "Class Field Theory", and on the other hand Jaulent has developed ℓ-adic class field theory in his article "Théorie ℓ-adique du corps des classes". The question is to know whether it is possible to deduce ℓ-adic class field theory from abstract class field theory, which requires in both cases (local case and global case) to define the degree map, the G-module, the valuation and to prove class field axiom.*

Key words: class field theory

Introduction:

The ℓ-adic class field theory, developed by Jaulent, claims, in the local case, the existence of an isomorphism between the Galois group of the maximal and abelian pro-ℓ-extension of a local field $K_{\mathfrak{p}}$ and the ℓ-adification of the multiplicative group of this local field; in the global case the existence of an isomorphism between the Galois group of the maximal and abelian pro-ℓ-extension of a number field K and the ℓ-adification of the group of ideles. The goal is to formalize this theory, following Neukirch. It requires to define the degree map, the G-module and the valuation in the local and in the global case. Then it requires to check that the valuations are henselian with respect to the degree map, and to prove in each case the class field axiom.

Contents

1 Preliminary

1.1 Notations

Let's introduce the notations:

For a local field : $K_\mathfrak{p}$

$\mathcal{R}_{K_\mathfrak{p}} = \varprojlim_k K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times \ell^k}$: the ℓ-adification of the multiplicative group of a local field

$\mathcal{U}_{K_\mathfrak{p}} = \varprojlim_k U_\mathfrak{p} / U_\mathfrak{p}^{\ell^k}$: the ℓ-adification of the group of units $U_\mathfrak{p}$ of $K_\mathfrak{p}$

$\mu_\mathfrak{p}$: the ℓ- Sylow subgroup of the group of roots of units

For a number field : K

$\mathcal{R}_K = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$: the ℓ-group of principal ideles

$\mathcal{J}_K = \prod_{\mathfrak{p} \in Pl_K}^{res} \mathcal{R}_{K_\mathfrak{p}}$: the ℓ-group of ideles K

$\mathcal{U}_K = \prod_{\mathfrak{p} \in Pl_K} \mathcal{U}_{K_\mathfrak{p}}$: the subgroup of units

$\mathcal{C}_K = \mathcal{J}_K / \mathcal{R}_K$: the idele class ℓ-group

1.2 The $\mathbb{Z}_\ell$-cohomology

As we focus on $\mathbb{Z}_\ell$-modules, we will use the following cohomology.

Definition The starting point is a $\mathbb{Z}[G]$ projective resolution where G is a ℓ-group:

$$F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

Applying the functor $\mathrm{Hom}_G(., \mathbb{Z}_\ell \otimes A)$ we obtain:

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell, \mathbb{Z}_\ell \otimes A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_0, \mathbb{Z}_\ell \otimes A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_1, \mathbb{Z}_\ell \otimes A) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell \ F_{n-1}, \mathbb{Z}_\ell \otimes A) \xrightarrow{\delta'_{n-1}} \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_n, \mathbb{Z}_\ell \otimes A) \xrightarrow{\delta'_n} \mathrm{Hom}_G(\mathbb{Z}_\ell \ F_{n+1}, \mathbb{Z}_\ell \otimes A) \cdots$$

We will denote $\mathrm{H}_\ell^n(G, \mathbb{Z}_\ell \otimes A) = \mathrm{Ker}\delta'_n / \mathrm{Im}\delta'_{n-1}$.

Theorem 1.2.1. *If G is a ℓ-group, and A a G-module then:*

$$H_\ell^i(G, \mathbb{Z}_\ell \otimes A) = \mathbb{Z}_\ell \otimes H^i(G, A)$$

Proof. We start with the $\mathbb{Z}[G]$ projective resolution:

$$F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

Applying the functor $\mathrm{Hom}_G(., A)$ we get:

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_G(F_0, A) \longrightarrow \mathrm{Hom}_G(F_1, A) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Hom}_G(F_{n-1}, A) \xrightarrow{\delta_{n-1}} \mathrm{Hom}_G(F_n, A) \xrightarrow{\delta_n} \mathrm{Hom}_G(F_{n+1}, A) \longrightarrow \cdots$$

So:

$$\mathrm{H}^n(G, A) = \mathrm{Ker}\delta_n / \mathrm{Im}\delta_{n-1}.$$

But the $\mathbb{Z}[G]$ projective resolution is an exact sequence, using the fact that $\mathbb{Z}_\ell$ is a flat module (cf [Li]), we then obtain:

$$\mathbb{Z}_\ell \otimes F_n \longrightarrow \mathbb{Z}_\ell \otimes F_{n-1} \longrightarrow \cdots \longrightarrow \mathbb{Z}_\ell \otimes F_1 \longrightarrow \mathbb{Z}_\ell \otimes F_0 \longrightarrow \mathbb{Z}_\ell \longrightarrow 0.$$

Applying now the functor $\mathrm{Hom}_G(., \mathbb{Z}_\ell \otimes A)$ we get:

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell, \mathbb{Z}_\ell \otimes A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_0, \mathbb{Z}_\ell \otimes A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_1, \mathbb{Z}_\ell \otimes A) \longrightarrow \cdots \longrightarrow$$
$$\mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_{n-1}, \mathbb{Z}_\ell \otimes A) \xrightarrow{\delta'_{n-1}} \mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_n, \mathbb{Z}_\ell \otimes A) \xrightarrow{\delta'_n} \cdots$$

So by definition

$$\mathrm{H}^n_\ell(G, \mathbb{Z}_\ell \otimes A) = \mathrm{Ker}\delta'_n / \mathrm{Im}\delta'_{n-1}.$$

Yet

$$\mathrm{Hom}_G(\mathbb{Z}_\ell \otimes F_i, \mathbb{Z}_\ell \otimes A) = \mathbb{Z}_\ell \otimes \mathrm{Hom}_G(G, A)$$

as in the projective resolution we can choose the F_i free: and using the additivity of the functor $\mathrm{Hom}_G(., A)$ it suffices to check the property on $\mathbb{Z}[G]$; but

$$\mathrm{Hom}_G(\mathbb{Z}[G], A) \simeq A \text{and} \quad \mathrm{Hom}_G(\mathbb{Z}_\ell[G], \mathbb{Z}_\ell \otimes A) \simeq \mathbb{Z}_\ell \otimes A.$$

Moreover

$$\mathrm{Ker}\delta'_n = \mathbb{Z}_\ell \otimes \mathrm{Ker}\delta_n \text{and} \quad \mathrm{Im}\delta'_{n-1} = \mathbb{Z}_\ell \otimes \mathrm{Im}\delta_{n-1}.$$

Indeed let's consider the following maps $u: \ M \longrightarrow N \ u' : \mathbb{Z}_\ell \otimes M \longrightarrow \mathbb{Z}_\ell \otimes N$; so we have this exact sequence:

$$0 \longrightarrow \mathrm{Ker}(u) \longrightarrow M \longrightarrow \mathrm{Im}(u) \longrightarrow 0.$$

then using the fact that $\mathbb{Z}_\ell$ is a flat module:

$$0 \longrightarrow \mathbb{Z}_\ell \otimes \mathrm{Ker}(u) \longrightarrow \mathbb{Z}_\ell \otimes M \longrightarrow \mathbb{Z}_\ell \otimes \mathrm{Im}(u) \longrightarrow 0.$$

Moreover we have $\mathrm{Im}(u) \subset N$ and as $\mathbb{Z}_\ell$ is a flat module, we also have $\mathbb{Z}_\ell \otimes \mathrm{Im}(u) \subset \mathbb{Z}_\ell \otimes N$, so we get the previous result. Finally,

$$\mathrm{Ker}\delta'_n / \mathrm{Im}\delta'_{n-1} \simeq \mathbb{Z}_\ell \otimes (\mathrm{Ker}\delta_n / \mathrm{Im}\delta_{n-1}).$$

□

2 Local ℓ-adic class field theory

2.1 Introduction

In the following ℓ is a fixed prime number. The fundamental local ℓ-adic theorem is the following:

Theorem 2.1.1 (Ja1). *Given a local field $K_\mathfrak{p}$, the reciprocity map induces an isomorphism of topological $\mathbb{Z}_\ell$-modules between $\mathcal{R}_{K_\mathfrak{p}} = \varprojlim_k K_\mathfrak{p}^\times / K_\mathfrak{p}^{\ell^k}$ and the Galois group $\mathcal{D}_\mathfrak{p} = Gal(K_\mathfrak{p}^{ab}/K_\mathfrak{p})$ of the maximal and abelian pro-ℓ-extension of $K_\mathfrak{p}$. Trough this isomorphism, the image of the inertia sub-group $\mathcal{I}_\mathfrak{p}$ is the sub-group of units $\mathcal{U}_{K_\mathfrak{p}}$ of $\mathcal{R}_{K_\mathfrak{p}}$. The reciprocity map induces a one to one correspondence between closed sub-modules of $\mathcal{R}_{K\mathfrak{p}}$ and abelian ℓ-extensions of $K_\mathfrak{p}$: in this correspondence, finite abelian ℓ-extensions are associated to closed sub-modules of finite index of $\mathcal{R}_{K_\mathfrak{p}}$; it means to open sub-modules of $\mathcal{R}_{K_\mathfrak{p}}$.*

The purpose is to prove the existence of the local reciprocity map using Neukirch's abstract class field theory.

We consider the following general framework: G is an abstract profinite group, whose closed subgroups are denoted by G_K, those indices K are called "fields".

1. We denote by k the field such that $G_k = G$,
2. We denote by $\bar{k}$ the field such that $G_{\bar{k}} = \{1\}$,
3. If $G_L \subset G_K$, we write $K \subset L$,
4. L/K is said finite if G_L is open (it means closed of finite index) in G_K; the degree of $[L : K]$ is then defined by $[L : K] = (G_K : G_L)$,
5. We write $K = \prod K_i$ for $G_K = \cap_i G_{K_i}$,
6. We write $K = \cap K_i$ for $G_K = \prod_i G_{K_i}$, it means that G_K is topologically generated by G_{K_i},
7. If G_L is normal in G_K we say that L/K is a Galois extension and we write $\mathrm{Gal}(L/K) = G_K/G_L$,
8. If K is a finite extension k we define $\tilde{K} = K \cdot \tilde{k}$ (where $\tilde{k}$ is defined above).

The first point of the theory is **a homomorphism called the degree**: the degree is a continuous and surjective homomorphism: $\deg : \ G \longrightarrow \widehat{\mathbb{Z}}$; the kernel of the degree is a subgroup of G denoted by $G_{\tilde{k}} = I$ such that $G/G_{\tilde{k}} \simeq \widehat{\mathbb{Z}}$. We can restrict the degree to G_K and define:

$$f_K = (\mathbb{Z} : \deg(G_K)) \qquad e_K = (G_{\tilde{k}} : G_{\tilde{K}}) \qquad I_K = G_{\tilde{K}}.$$

If L/K is an extension we put:

$$f_{L/K} = (\deg(G_K) : \deg(G_L)) \qquad e_{L/K} = (I_K : I_L)$$

which are called the inertia degree and the ramification index. They check the following relations:

$$f_{L/K} = f_L/f_K \qquad [L : K] = e_{L/K} \cdot f_{L/K}.$$

The second point of the theory requires **a G module and a henselian valuation with respect to the degree** : for Neukirch (Algebraic Number Theory p 276) a multiplicative G module A is an abelian multiplicative group on which G operates through its automorphisms.

$$\begin{array}{cccc} \sigma & : & A & \rightarrow & A \\ & & a & \mapsto & a^\sigma \end{array}$$

This action satisfies the following rules:

(i) $a^1 = a$

(ii) $(ab)^\sigma = a^\sigma \cdot b^\sigma$

(iii) $a^{\sigma \cdot \tau} = (a^\sigma)^\tau$

(iv) $A = \bigcup_{[K:k]<\infty} A_K$ where $A_K = \{a \in A \mid a^\sigma = a, \forall \sigma \in G_K\} = A^{G_K}$ and where K runs trough all finite extensions of k. This condition (iv) is equivalent to say that G acts continuously on A which means that the following application

$$\begin{array}{cccc} \phi & : & G \times A & \rightarrow & A \\ & & (\sigma, a) & \mapsto & a^\sigma \end{array}$$

is continuous if A is equipped with the discrete topology.

We denote by $A_K$the elements of the G-module A which are fixed under the action of G_K a subgroup of G. For Neukirch (Algebraic Number Theory p 288), a henselian valuation of A_k with respect to $\deg :\ G \to \widehat{\mathbb{Z}}$ is a homomorphism checking the following properties:

(i) $v(A_k) = Z$ such that $\mathbb{Z} \subset Z$ et $Z/n \cdot Z \simeq \mathbb{Z}/n \cdot \mathbb{Z}$ for all n

(ii) $v(N_{K/k}A_K) = f_K.Z$ for all extension K of k. The norm map, which goes to the G-module A_K in A_k, is defined by:

$$N_{K/k}(a) = \textstyle\prod_\sigma a^\sigma$$

where σ runs through a representative coset of G_K/G_L.

The third point of the theory is **the class field axiom**:

Axiom 1. *For all cyclic extension L/K, we get:*

$$|H^i(G(L/K), A_L| = \begin{cases} [L:K] & \textit{for } i = 0 \\ 1 & \textit{for } i = -1 \end{cases}$$

In this context Neukirch proves the following fundamental theorem:

Theorem 2.1.2. *If L/K is a finite Galois extension the homomorphism*

$$\begin{array}{cccc} r_{L/K} & : & G(L/K)^{ab} & \to & A_K/N_{L/K}(A_L) \\ & & \sigma & \mapsto & N_{\Sigma/K}(\pi_\Sigma) \bmod N_{L/K}A_L \end{array}$$

where Σ is the fixed field of $\tilde{\sigma} \in Gal(\tilde{L}/K)$, (which is the Frobenius lift of σ) and π_Σ is a prime element of A_Σ is an isomorphism.

We know want to define the degree, the G-module and the henselian valuation in the context of ℓ-adic class field theory in order to obtain the reciprocity map.

2.2 The degree

We consider the following context: by definition a ℓ-extension is a Galois extension whose Galois group is a ℓ-group.

k is a local field, (we use this notation instead of $k_\mathfrak{p}$).

k^{nr} is the maximal unramified pro-ℓ-extension of k: the compositum of all unramified ℓ-extensions.

$\widehat{k}$ is the maximal pro-ℓ-extension of k: the compositum of ℓ-extensions.

$$\begin{tikzcd} \widehat{k} \arrow[d, dash] \\ k^{nr} \arrow[d, dash, "\mathbb{Z}_\ell"] \\ k \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

We write

$$G = \mathrm{Gal}(\widehat{k}/k)$$

Definition-Proposition

The degree map is defined by:

$$\begin{array}{cccc} \deg & : & G & \rightarrow & \mathbb{Z}_\ell \\ & & \phi & \mapsto & \phi_{|k^{nr}} \end{array}$$

Thus this is a surjective homomorphism. The kernel of this homomorphism is $G_{k^{nr}}$; we will denote $I = G_{k^{nr}}$ so,

$$G/I = G/G_{k^{nr}} \simeq \mathrm{Gal}(k^{nr}/k) \simeq \mathbb{Z}_\ell$$

Proof. $\phi \in G$, ϕ is a k-automorphism of $\widehat{k}$, whose restriction to k^{nr} defines an element of $\mathbb{Z}_\ell$, due to the following homomorphism

$$\mathrm{Gal}(\widehat{k}/k) \simeq \mathbb{Z}_\ell.$$

The surjectivity is due to the fact that $\mathrm{Gal}(k^{nr}/k) \simeq G/G_{k^{nr}}$. □

Definitions: Given a finite ℓ-extension$K$ of k ,we put:

$$f_K = (\mathbb{Z}_\ell : \deg(G_K)) \qquad \& \qquad e_K = (I : I_K)$$

$$I_K = I \cap G_K = G_{k^{nr}} \cap G_K = G_{K \cdot k^{nr}} = G_{K^{nr}}$$

$$\begin{tikzcd} k^{nr} \arrow[r, dash] \arrow[d, dash] & K^{nr} \arrow[d, dash, "\mathbb{Z}_\ell"] \\ k \arrow[r, dash] & K \end{tikzcd}$$

Definitions: If L/K is a finite ℓ-extension we put:

$$f_{L/K} = (\deg(G_K) : \deg(G_L)); e_{L/K} = (I_K : I_L)$$

Proposition 2.2.1. *We have the following fundamental relations:*

$$f_{L/K} = f_L / f_K$$

$$e_{L/K} \cdot f_{L/K} = [L : K]$$

Proof. Neukirch p. 286. □

2.3 The G-module

We consider the following G-module:

$$A = \varinjlim_{L_\mathfrak{P}} \mathcal{R}_{L_\mathfrak{P}}$$

where $L_\mathfrak{P}$ runs through all finite extensions of $K_\mathfrak{p}$, where $\mathcal{R}_{L_\mathfrak{P}} = \varprojlim_k L_\mathfrak{P}^\times / L_\mathfrak{P}^{\times \ell^k}$. It can be canonically identified to

$$A = \bigcup_{[L_\mathfrak{P}:K_\mathfrak{p}]<\infty} \mathcal{R}_{L_\mathfrak{P}}.$$

If $L_\mathfrak{P}$ is a finite extension of $K_\mathfrak{p}$,

$$A_{L_\mathfrak{P}} = \mathcal{R}_{L_\mathfrak{P}}$$

is our $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ module. (The group acts components by components.)

2.4 The valuation

In ℓ-adic class filed theory, the degree is a homomorphism from G to $\mathbb{Z}_\ell$, and the valuation v is a homomorphism from A_k to $\mathbb{Z}_\ell$. In this part, we denote by $K_\mathfrak{p}$ a local field.

Proposition 2.4.1. *For a finite extension $L_\mathfrak{P}$ of a local field $K_\mathfrak{p}$*

$$A_{L_\mathfrak{P}} = \mathcal{R}_{L_\mathfrak{P}} = \varprojlim_k L_\mathfrak{P}^\times / L_\mathfrak{P}^{\times \ell^k}$$

is our $Gal(L_\mathfrak{P}/k)$-module. Due to the explicit expression of $\mathcal{R}_{L_\mathfrak{P}}$:

$$\mathcal{R}_{L_\mathfrak{P}} \simeq U_\mathfrak{P}^1 \cdot \pi_\mathfrak{P}^{\mathbb{Z}_\ell} \text{ if } \mathfrak{P}|\ell$$

$$\mathcal{R}_{L_\mathfrak{P}} \simeq \mu_\mathfrak{P} \cdot \pi_\mathfrak{P}^{\mathbb{Z}_\ell} \text{ if } \mathfrak{P} \not| \ell$$

the valuation v_L gives the power in $\mathbb{Z}_\ell$ of the uniformising element. This valuation is henselian with respect to the degree, according to the previous definition.

Proof. For a local field $K_\mathfrak{p}$ the valuation $v_\mathfrak{p}$ is linked to the explicit expression of $\mathcal{R}_{K_\mathfrak{p}}$ $v_\mathfrak{p} : \mathcal{R}_{K_\mathfrak{p}} \longrightarrow \mathbb{Z}_\ell$ where

$$\mathcal{R}_{K_\mathfrak{p}} \simeq \mu_\mathfrak{p} \cdot \pi_\mathfrak{p}^{\mathbb{Z}_\ell} \text{ if } \mathfrak{p} \not| \ell$$

$$\mathcal{R}_{K_\mathfrak{p}} \simeq U_\mathfrak{p}^1 \cdot \pi_\mathfrak{p}^{\mathbb{Z}_\ell} \text{ if } \mathfrak{p}|\ell$$

Thus $v_\mathfrak{p}$ is a surjective homomorphism:

$$v_\mathfrak{p}(\mathcal{R}_{K_\mathfrak{p}}) = \mathbb{Z}_\ell; \text{ moreover } \forall n \in \mathbb{N} \text{ we get } \mathbb{Z}_\ell/n.\mathbb{Z}_\ell \simeq \mathbb{Z}/n.\mathbb{Z}.$$

The first point (i) of the definition is checked. Moreover $v_L : \mathcal{R}_{L_\mathfrak{P}} \longrightarrow \mathbb{Z}_\ell$ can also be viewed as the continuation of the usual normalized valuation of $L_\mathfrak{P}$, denoted by w_L. In fact, we have the following commutative diagram:

$$\begin{tikzcd} L_\mathfrak{P}^\times \arrow[r] \arrow[d, "w_\mathfrak{P}"'] & \mathcal{R}_{L_\mathfrak{P}} \arrow[d, "v_\mathfrak{P}"] \\ \mathbb{Z} \arrow[r] & \mathbb{Z}_\ell \end{tikzcd}$$

If $L_\mathfrak{P}$ is an extension of a local field $K_\mathfrak{p}$,

$$\begin{tikzcd} L_\mathfrak{P} \arrow[d, dash] \\ K_\mathfrak{p} \end{tikzcd}$$

If $v_\mathfrak{p}$ is the valuation on $\mathcal{R}_{K_\mathfrak{p}}$, we denote by $w_\mathfrak{p}$ the usual normalized valuation on $K_\mathfrak{p}$, and we get the following commutative diagram:

$$\begin{tikzcd} K_\mathfrak{p} \arrow[r] \arrow[d, "w_\mathfrak{p}"'] & \mathcal{R}_{K_\mathfrak{p}} \arrow[d, "v_\mathfrak{p}"] \\ \mathbb{Z} \arrow[r] & \mathbb{Z}_\ell \end{tikzcd}$$

Due to properties to local fields, $w_\mathfrak{p}$ extends uniquely to $L_\mathfrak{P}$ by: $\frac{1}{[L_\mathfrak{P}:K_\mathfrak{p}]}(w_\mathfrak{p} \circ N_{L_\mathfrak{P}/K_\mathfrak{p}})$ and thus $v_\mathfrak{p}$ extends uniquely to $L_\mathfrak{P}$. As $\frac{1}{e_{L_\mathfrak{P}/K_\mathfrak{p}}} \cdot w_\mathfrak{P}$ is the continuation of $w_\mathfrak{p}$, we get:

$$\frac{1}{e_{L_\mathfrak{P}/K_\mathfrak{p}}} \cdot v_\mathfrak{P}(\mathcal{R}_{L_\mathfrak{P}}) = \frac{1}{[L_\mathfrak{P} : K_\mathfrak{p}]} \cdot v_\mathfrak{p}(N_{L_\mathfrak{P}/K_\mathfrak{p}} \mathcal{R}_{K_\mathfrak{p}}) = \frac{1}{e_{L_\mathfrak{P}/K_\mathfrak{p}} . f_{L_\mathfrak{P}/K_\mathfrak{p}}} \cdot v_\mathfrak{p}(N_{L_\mathfrak{P}/K_\mathfrak{p}} \mathcal{R}_k)$$

So we deduce that:

$$f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \cdot v_{\mathfrak{P}}(\mathcal{R}_{L_{\mathfrak{P}}}) = v_k(N_{L_{\mathfrak{P}}/k}\mathcal{R}_k)$$

Yet we have the relation $f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = f_{L_{\mathfrak{P}}}/f_{K_{\mathfrak{p}}}$, and due to the definition of $f_{K_{\mathfrak{p}}}$ we have $f_{K_{\mathfrak{p}}} = (\mathbb{Z}_\ell : d(G_{K_{\mathfrak{p}}})) = 1$ as the degree is surjective. Finally, we get:

$$f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \cdot v_{\mathfrak{P}}(\mathcal{R}_{L_{\mathfrak{P}}}) = f_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} \cdot \mathbb{Z}_\ell = v_{\mathfrak{p}}(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\mathcal{R}_{K_{\mathfrak{p}}})$$

for all finite extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$, the second point point (ii) is also checked. □

2.5 The class field axiom

Theorem 2.5.1. *For all cyclic ℓ-extension $L_{\mathfrak{P}}$ of a local field $K_{\mathfrak{p}}$ we have*

$$|H^i_\ell(G(L_{\mathfrak{P}}/K_p), \mathcal{R}_{L_{\mathfrak{P}}})| = \begin{cases} [L_{\mathfrak{P}} : K_p] & \text{for } i = 0 \\ 1 & \text{for } i = 1 \end{cases}$$

Proof. Let's denote $G = G(L_{\mathfrak{P}}/K_p)$

First step: We are going to prove that $h(G, \mathcal{R}_{L_{\mathfrak{P}}}) = [L_{\mathfrak{P}} : K_p]$. Let's consider the following exact sequence, where $\mathbb{Z}_\ell$ is considered as a trivial G-module.

$$1 \longrightarrow \mathcal{U}_{L_{\mathfrak{P}}} \longrightarrow \mathcal{R}_{L_{\mathfrak{P}}} \xrightarrow{v_L} \mathbb{Z}_\ell \longrightarrow 1.$$

$$\mathcal{R}_{L_{\mathfrak{P}}} \simeq U^1_{\mathfrak{P}} \cdot \pi_{\mathfrak{P}}^{\mathbb{Z}_\ell} \text{ and } \mathcal{U}_{L_{\mathfrak{P}}} \simeq U^1_{\mathfrak{P}} \text{ if } \mathfrak{P}|\ell$$

$$\mathcal{R}_{L_{\mathfrak{P}}} = \mu_{\mathfrak{P}} \cdot \pi_{\mathfrak{P}}^{\mathbb{Z}_\ell} \text{ and } \mathcal{U}_{L_{\mathfrak{P}}} \simeq \mu_{\mathfrak{P}} \text{ if } \mathfrak{P} \not|\ell$$

where $\mu_{\mathfrak{P}}$ is the ℓ Sylow subgroup of the group of roots of units in $L_{\mathfrak{P}}$, where $U^1_{\mathfrak{P}}$ is the subgroup of principal units of $L_{\mathfrak{P}}$, where v_L is the valuation obtained with the explicit expression of $\mathcal{R}_{L_{\mathfrak{P}}}$. As G is a finite cyclic group, we get using the property of the Herbrand's quotient

$$h(G, \mathcal{R}_{L_{\mathfrak{P}}}) = h(G, \mathcal{U}_{L_{\mathfrak{P}}}) \cdot h(G, \mathbb{Z}_\ell)$$

And $\mathbb{Z}_\ell$ is considered as a trivial G-module:

$$\mathrm{H}^0(G, \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell/(|G| \cdot \mathbb{Z}_\ell) \text{ and } \mathrm{H}^{-1}(G, \mathbb{Z}_\ell) \text{ is trivial. Thus } h(G, \mathbb{Z}_\ell) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}].$$

Consequently it suffices to show that $h(G, \mathcal{U}_{L_{\mathfrak{P}}}) = 1$.

If $\mathfrak{P} \not|\ell$: as $\mu_{\mathfrak{P}}$ is the ℓ-Sylow subgroup of the group of units in $L_{\mathfrak{P}}$ it is a finite group, so a finite G-module; and using Herbrand's property we get $h(G, \mathcal{U}_{L_{\mathfrak{P}}}) = 1$.

If $\mathfrak{P}|\ell$: due to Neukirch's proof (p. 40 Class Field Theory) $h(G, U_{L_{\mathfrak{P}}}) = 1$ and with the following exact sequence:

$$1 \longrightarrow U^1_{L_{\mathfrak{P}}} \longrightarrow U_{L_{\mathfrak{P}}} \longrightarrow U_{L_{\mathfrak{P}}}/U^1_{L_{\mathfrak{P}}} \longrightarrow 1$$

By Hensel's lemma $U_{L_{\mathfrak{P}}}/U^1_{L_{\mathfrak{P}}} \simeq \kappa^*$ where κ is the residue field. So $h(G, U_{L_{\mathfrak{P}}}) = h(G, U^1_{L_{\mathfrak{P}}}) \cdot h(G, U_{L_{\mathfrak{P}}}/U^1_{L_{\mathfrak{P}}})$. In this case we also obtain, $h(G, U^1_{L_{\mathfrak{P}}}) = 1$. In both cases, we have $h(G, \mathcal{U}_{L_{\mathfrak{P}}}) = 1$.

Step 2: Let's show that $h(G, L_{\mathfrak{P}}^\times/L_{\mathfrak{P}}^{\times div}) = [L_{\mathfrak{P}} : K_p]$

Hensel's lemma gives the structure of the multiplicative group:

$$L_{\mathfrak{P}}^\times \simeq \mu^0_{\mathfrak{P}} \cdot U^1_{\mathfrak{P}} \cdot \pi_{\mathfrak{P}}^{\mathbb{Z}} \text{ et } \mu^0_{\mathfrak{P}} \simeq \mu_{\mathfrak{P}} \cdot \mu'_{\mathfrak{P}}$$

where $\mu_{\mathfrak{P}}$ is the ℓ-Sylow subgroup of the group of roots of units and $\mu_{\mathfrak{P}}^0$ is its ℓ-divisible part.

case 1: If $\mathfrak{P} \not| \ell$ then $\mathfrak{P}$ and ℓ are distinct, so ℓ is invertible in $\mathbb{Z}_\ell$ thus $U_{L_{\mathfrak{P}}}^1$ is ℓ-divisible. Finally $\mu_{\mathfrak{P}}^{'} \cdot U_{\mathfrak{P}}^1$ is ℓ-divisible. As $h(G, \mu_{\mathfrak{P}}^{'} \cdot U_{\mathfrak{P}}^1) = h(G, \mu_{\mathfrak{P}}^{'}) \cdot h(G, U_{\mathfrak{P}}^1)$; and because $\mu_{\mathfrak{P}}^{'}$ is a finite group so a finite G- module $h(G, U_{\mathfrak{P}}^1) = 1$; consequently:

$$h(G, \mu_{\mathfrak{P}}^{'} \cdot U_{\mathfrak{P}}^1) = 1.$$

Moreover, if A is a G-module by definition $\mathrm{H}^0(G, A) = \mathrm{Ker}(\delta)/\mathrm{Im}(\nu)$ where

$$\begin{array}{ccccc} \delta & : & A & \rightarrow & A \\ & & a & \mapsto & (\sigma - 1)a \end{array} \qquad \begin{array}{ccccc} \nu & : & A & \rightarrow & A \\ & & a & \mapsto & (1 + \sigma + \cdots + \sigma^{[L_{\mathfrak{P}} : K_p]})a \end{array}$$

If $a \in \mathrm{Ker}(\delta)$ and $a \in L_{\mathfrak{P}}^{div}$ then $a \in (\mu_{\mathfrak{P}}^{'} \cdot U_{\mathfrak{P}}^1)^G$ but the extension is a Galois extension so:

$$(\mu_{\mathfrak{P}}^{'} \cdot U_{\mathfrak{P}}^1)^G = (\mu_{\mathfrak{p}}^{'} \cdot U_{\mathfrak{p}}^1)$$

where $K_{\mathfrak{p}}^\times \simeq \mu_{\mathfrak{p}} \cdot \mu_{\mathfrak{p}}^{'} \cdot U_{\mathfrak{p}}^1 \cdot \pi_{\mathfrak{p}}^{\mathbb{Z}}$. Consequently $a \in \mu_{\mathfrak{p}}^{'} \cdot U_{\mathfrak{p}}^1$, which means to the ℓ-divisible part of $K_{\mathfrak{p}}^\times$ and we can choose $b \in K_{\mathfrak{p}}^\times$ such that $a = b^{\ell^{[L_{\mathfrak{P}}:K_p]}} = N(b)$. It follows that $\mathrm{H}^0(G, L_{\mathfrak{P}}^{\times div}) = 1$, as $h(G, L_{\mathfrak{P}}^{\times div}) = 1$ we finally get $\mathrm{H}^1(G, L_{\mathfrak{P}}^{\times div}) = 1$. Let's consider the following exact sequence:

$$1 \longrightarrow L_{\mathfrak{P}}^{\times div} \longrightarrow L_{\mathfrak{P}}^\times \longrightarrow L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{\times div} \longrightarrow 1$$

As G is a cyclic group, we obtain the following Herbrand's hexagon:

$$\begin{tikzcd}
& \mathrm{H}^0(G, L_{\mathfrak{P}}^{\times div}) \arrow[r] & \mathrm{H}^0(G, L_{\mathfrak{P}}^\times) \arrow[dr] & \\
\mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{\times div}) \arrow[ur] & & & \mathrm{H}^0(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{div}) \arrow[dl] \\
& \mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times) \arrow[ul] & \mathrm{H}^{-1}(G, L_{\mathfrak{P}}^{div}) \arrow[l] &
\end{tikzcd}$$

And we extract the following exact sub-sequence:

$$1 \longrightarrow \mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times) \longrightarrow \mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{\times div}) \longrightarrow 1$$

Hilbert's 90 theorem and the fact that G is a cyclic group lead to $\mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times) = 1$ So we deduce:

$$\mathrm{H}^{-1}(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{\times div}) = 1$$

Moreover we also have the following exact sequence:

$$1 \longrightarrow \mathrm{H}^0(G, L_{\mathfrak{P}}^\times) \longrightarrow \mathrm{H}^0(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{\times div}) \longrightarrow 1$$

Using the local class field axiom we deduce that:

$$\mathrm{H}^0(G, L_{\mathfrak{P}}^\times) \simeq \mathrm{H}^0(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{div}) \text{ so } |\mathrm{H}^0(G, L_{\mathfrak{P}}^\times)| = |\mathrm{H}^0(G, L_{\mathfrak{P}}^\times / L_{\mathfrak{P}}^{div})| = [L_{\mathfrak{P}} : K_p]$$

So in this first case:

$$h(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}) = [L_{\mathfrak{P}} : K_p]$$

case 2: If $\mathfrak{P}|\ell$ the group $\mu_{\mathfrak{P}}^0$ is ℓ-divisible, and as the group of principal units is a noetherian $\mathbb{Z}_\ell$-module, it is isomorphic to the inverse limit of its finite quotients.

$$L_{\mathfrak{P}}^{\times} \simeq \underbrace{\mu_{\mathfrak{P}}^0}_{div\,part} \cdot U_{\mathfrak{P}}^1 \cdot \pi_{\mathfrak{P}}^{\mathbb{Z}}$$

And $\mu_{\mathfrak{P}}^0$ is a finite group, so $h(G, \mu_{\mathfrak{P}}^0) = 1$; using the same arguments as before we finally obtain that $\mathrm{H}^0(G, L_{\mathfrak{P}}^{\times div})$ is trivial.

Consequently in both cases:

$$h(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}) = [L_{\mathfrak{P}} : K_p]$$

Step 3: Conclusion

By step 1: $h(G, \mathcal{R}_{L_{\mathfrak{P}}}) = [L_{\mathfrak{P}} : K_p]$.

By step 2: $h(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}) = [L_{\mathfrak{P}} : K_p]$.

Moreover, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a cyclic ℓ-extension of a local field: so it checks the class field axiom: $h(G, L_{\mathfrak{P}}^{\times}) = [L_{\mathfrak{P}} : K_p]$. As $\mathcal{R}_{L_{\mathfrak{P}}} = \varprojlim_k L_{\mathfrak{P}}^{\times} / L_{\mathfrak{P}}^{\times \ell^k} = \mathbb{Z}_\ell \otimes L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}$ and as by property $\mathrm{H}^0(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}) = \mathrm{H}_\ell^0(G, \mathcal{R}_{L_{\mathfrak{P}}})$ we obtain

$$|\mathrm{H}^0(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div})| = |\mathrm{H}_\ell^0(G, \mathcal{R}_{L_{\mathfrak{P}}})| = [L_{\mathfrak{P}} : K_p]$$

Consequently

$$h(G, \mathcal{R}_{L_{\mathfrak{P}}}) = h(G, L_{\mathfrak{P}}^{\times}/L_{\mathfrak{P}}^{\times div}) = [L_{\mathfrak{P}} : K_p]$$

so we deduce:

$$\mathrm{H}_\ell^{-1}(G, \mathcal{R}_{L_{\mathfrak{P}}}) = 1.$$

And as G is cyclic, we get

$$\mathrm{H}_\ell^1(G, \mathcal{R}_{L_{\mathfrak{P}}}) = 1.$$

□

2.6 Conclusion

Theorem 2.6.1. (deg, v) *is a class field pair, and* $A_K = \mathcal{R}_{K_{\mathfrak{p}}}$ *checking the class field axiom, then for all Galois* ℓ*-extension* $L_{\mathfrak{P}}$ *of a local field* $K_{\mathfrak{p}}$ *we get the following isomorphism:*

$$Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}})^{ab} \simeq \mathcal{R}_{K_{\mathfrak{p}}}/N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\mathcal{R}_{L_{\mathfrak{P}}}.$$

In particular for all abelian ℓ*-extension of a local field:*

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \simeq \mathcal{R}_{K_{\mathfrak{p}}}/N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\mathcal{R}_{L_{\mathfrak{P}}}.$$

We then get a one to one correspondence between finite and abelian ℓ*-extensions of a local field and the closed subgroups of finite index of* $\mathcal{R}_{K_{\mathfrak{p}}}$*.*

3 Global ℓ-adic class field theory

3.1 Introduction

The fundamental global ℓ-adic class field theory is the following:

Theorem 3.1.1 (Ja1). *Given a number field K, the reciprocity map induces a continuous isomorphism between the ℓ-group of ideles $\mathcal{J}_K$ of K and the Galois group $G_K^{ab} = Gal(K^{ab}/K)$ of the maximal abelian pro-ℓ-extension of K. The kernel of this morphism is the subgroup $\mathcal{R}_K$ of principal ideles. In this correspondence, the decomposition subgroup $\mathcal{D}_\mathfrak{p}$ of a prime $\mathfrak{p}$ of K is the image in G_K^{ab} of the sub-group $\mathcal{R}_{K_\mathfrak{p}}$ of $\mathcal{J}_K$; and the inertia sub-group $\mathcal{I}_\mathfrak{p}$ is the image of the subgroup of units $\mathcal{U}_{K_\mathfrak{p}}$ of $\mathcal{R}_{K_\mathfrak{p}}$. The reciprocity map leads to a one to one correspondence between closed sub-modules of $\mathcal{J}_K$ containing $\mathcal{R}_K$ and abelian ℓ-extensions of K. Each sub-extension of K^{ab} is the fixed field of a unique closed sub-module of $\mathcal{J}_K$ containing $\mathcal{R}_K$. In this correspondence, finite and abelian ℓ-extensions of K are associated to closed sub-modules of finite index of $\mathcal{J}_K$ containing $\mathcal{R}_K$, it means to open sub-modules of $\mathcal{J}_K$ containing $\mathcal{R}_K$.*

The goal is to prove the existence of the reciprocity map in the global case using Neukirch's abstract theory.

3.2 The class field axiom

Proposition 3.2.1. *If L/K is a finite extension then the injection of $\mathcal{J}_K$ in $\mathcal{J}_L$ induces an injection between their idele class ℓ-groups:*

$$\begin{array}{ccc} \mathcal{C}_K & \longrightarrow & \mathcal{C}_L \\ \alpha \cdot \mathcal{R}_K & \longmapsto & \alpha \cdot \mathcal{R}_L \end{array}$$

Proof. The injection of $\mathcal{J}_K$ in $\mathcal{J}_L$ sends $\mathcal{R}_K = \mathbb{Z}_\ell \otimes K^\times$ in $\mathcal{R}_L$

$$\begin{tikzcd} \mathcal{J}_K \arrow[r] \arrow[d] & \mathcal{J}_L \arrow[d] \\ \mathcal{J}_K/\mathcal{R}_K \arrow[r] & \mathcal{J}_L/\mathcal{R}_L \end{tikzcd}$$

This application leads to a homomorphism between $\mathcal{C}_K$ and $\mathcal{C}_L$. To show that this homomorphism is injective it suffices to show that $\mathcal{J}_K \cap \mathcal{R}_L = \mathcal{R}_K$. To do this, we consider M/K a finite Galois extension, whose Galois group is denoted by G, which contains L.

$$\begin{tikzcd} M \arrow[d, dash] \\ L \arrow[d, dash] \\ K \end{tikzcd}$$

so

$$\mathcal{J}_K \subseteq \mathcal{J}_L \subseteq \mathcal{J}_M$$

thus

$$\mathcal{J}_K \cap \mathcal{R}_L \subseteq \mathcal{J}_K \cap \mathcal{R}_M \subseteq (\mathcal{J}_K \cap \mathcal{R}_M)^G \subseteq \mathcal{J}_K \cap \mathcal{R}_M^G = \mathcal{J}_K \cap \mathcal{R}_K = \mathcal{R}_K.$$

□

Proposition 3.2.2. *If L/K is a finite Galois ℓ-extension, whose Galois group is denoted by $G = Gal(L/K)$, then $\mathcal{C}_L$ the idele class ℓ-group of L is canonically a G-module and:*

$$\mathcal{C}_L^G = \mathcal{C}_K.$$

Proof. $\mathcal{J}_L$ is a G-module which contains $\mathcal{R}_L$ as a sub-G-module, for all $\sigma \in G$, σ induces an automorphism of $\mathcal{C}_L$:

$$\begin{array}{ccc} \mathcal{C}_L & \to & \mathcal{C}_L \\ \alpha \cdot \mathcal{R}_L & \mapsto & \sigma(\alpha) \cdot \mathcal{R}_L \end{array}$$

We have the following exact sequence:

$$1 \longrightarrow \mathcal{R}_L \longrightarrow \mathcal{J}_L \longrightarrow \mathcal{C}_L \longrightarrow 1$$

But if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *is an exact sequence of* G*-modules then we have the following exact sequence:* $0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A)$

Consequently, applying this property here, we get:

$$1 \longrightarrow \mathcal{R}_L^G \longrightarrow \mathcal{J}_L^G \longrightarrow \mathcal{C}_L^G \longrightarrow \mathrm{H}^1(G, \mathcal{R}_L).$$

□

Let's show that $\mathcal{R}_L^G = \mathcal{R}_K$ using $\mathcal{R}_L = \mathbb{Z}_\ell \otimes L^\times$. Moreover we have the following property $\mathcal{J}_L^G = \mathcal{J}_K$. We also have to check that $\mathrm{H}^1(G, \mathcal{R}_L) = 1$.

Proposition 3.2.3. *If A is a G-module with G a cyclic group then we get: $(\mathbb{Z}_\ell \otimes A)^G = \mathbb{Z}_\ell \otimes A^G$, where A^G denotes the fixed points of A under the action of G.*

Proof. G is a cyclic group,

$$\mathrm{H}^0(G, A) = {}_\delta A / A^\nu \text{ et } \mathrm{H}^1(G, A) = {}_\nu A / A^\delta$$

(where we denote the kernel below on the left, and the image above on the right) so we have the following exact sequence:

$$1 \longrightarrow {}_\delta A \longrightarrow A \xrightarrow{\delta} A^\delta \longrightarrow 1$$

We use the fact that $\mathbb{Z}_\ell$ is a flat module to obtain the following other exact sequence:

$$1 \longrightarrow \mathbb{Z}_\ell \otimes {}_\delta A \longrightarrow \mathbb{Z}_\ell \otimes A \xrightarrow{\delta} \mathbb{Z}_\ell \otimes A^\delta \longrightarrow 1.$$

Denoting $\mathcal{A} = \mathbb{Z}_\ell \otimes A$ we get by the definition of the kernel of δ:

$${}_\delta\mathcal{A} = \mathbb{Z}_\ell \otimes {}_\delta A$$

and by definition ${}_\delta\mathcal{A} = {}_\delta(\mathbb{Z}_\ell \otimes A)$; as the fixed points are just the kernel of δ we get the result. □

Previous proof:

Due to the previous proposition, we get: $\mathcal{R}_L^G = \mathcal{R}_K$.
Due to the theorem 1.0.1 and 90 Hilbert's theorem, we have: $\mathrm{H}^1(G, \mathcal{R}_L) = 1$.
Consequently we get:

$$1 \longrightarrow \mathcal{R}_K \longrightarrow \mathcal{J}_K \longrightarrow \mathcal{C}_L^G \longrightarrow 1$$

so $\mathcal{C}_L^G = \mathcal{C}_K$.

Theorem 3.2.1. *The Herbrand quotient of the idele class ℓ-group. If L/K is a Galois cyclic ℓ-extension of finite degree ℓ^n, whose Galois group is $G = Gal(L/K)$ then*

$$h(G, \mathcal{C}_L) = \tfrac{|H^0(G,\mathcal{C}_L|}{|H^1(G,\mathcal{C}_L)|} = \ell^n.$$

In particular $(\mathcal{C}_K : N_{L/K}\mathcal{C}_L) \geq n$.

Proof: Step 1: If S is a set of primes big enough:

$$\mathcal{J}_K = \mathcal{J}_K^S \cdot \mathcal{R}_K$$

with

$$\mathcal{J}_K = \bigcup_S \mathcal{J}_K^S$$

and

$$\mathcal{J}_K^S = \prod_{\mathfrak{p}\in S} (\mathcal{R}_{K_\mathfrak{p}}) \prod_{\mathfrak{p}\notin S} (\mathcal{U}_{K_\mathfrak{p}})$$

where S runs through finite sets of primes of K. We are going to use the following topological direct sum:

$$\mathcal{J}_K = \mathcal{D}_K \oplus \mathcal{U}_K$$

where $\mathcal{D}_K$ is the ℓ-group of the classes of divisors of K, which can be identified to the $\mathbb{Z}_\ell$ multiplicative module built on $\pi_\mathfrak{p}$.

$$\mathcal{D}_K = \bigoplus_{\mathfrak{p}\not|\infty} \mathfrak{p}^{\mathbb{Z}_\ell} \bigoplus_{\mathfrak{p}|\infty} \mathfrak{p}^{\mathbb{Z}_\ell/2\cdot\mathbb{Z}_\ell}$$

Indeed we are going to consider this map:

$$\begin{array}{ccc} \mathcal{J}_K & \to & \mathcal{D}_K \\ \alpha = (\alpha_\mathfrak{p}) & \mapsto & \prod_{\mathfrak{p}\not|\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \end{array}$$

$\alpha_\mathfrak{p} \in \mathcal{R}_{K_\mathfrak{p}}$ et $v_\mathfrak{p}$ is the valuation on $\mathcal{R}_{K_\mathfrak{p}}$ which is just the power in $\mathbb{Z}_\ell$ of the uniformising element. This homomorphism is a a surjective one, whose kernel is: $\alpha \in \mathcal{J}_K$ such that $\forall \mathfrak{p} \not|\infty, v_\mathfrak{p}(\alpha_\mathfrak{p}) = 0$ i.e $\alpha_\mathfrak{p} \in \mathcal{U}_\mathfrak{p}$. The kernel is just $\mathcal{J}_K^{S_\infty}$. So we get the isomorphism:

$$\mathcal{J}_K / \mathcal{J}_K^{S_\infty} \simeq \mathcal{D}_K$$

If $\mathcal{P}_K$ is the ℓ-sub-group of principal divisors, which can be identified to the image of $\mathcal{R}_K$ in $\mathcal{D}_K$, we get:

$$\mathcal{R}_K \cdot \mathcal{J}_K^{S_\infty} / \mathcal{J}_K^{S_\infty} \simeq \mathcal{P}_K$$

And using the double quotient theorem:

$$\mathcal{J}_K / \mathcal{R}_K \cdot \mathcal{J}_K^{S_\infty} \simeq \mathcal{D}_K / \mathcal{P}_K$$

By [Ja 1 p.364] $\mathcal{D}_K/\mathcal{P}_K \simeq \mathcal{C}\ell_K$ can be identified to the ℓ-Sylow sub-group of the restricted class group. As $\mathcal{D}_K/\mathcal{P}_K$ is finite, we choose $a_1, a_2, \ldots, a_h$ cosets of each classes in $\mathcal{D}_K/\mathcal{P}_K$; $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ are the primes which divide $a_1, a_2, \ldots, a_h$. If S is a set of primes sufficiently big enough: it means containing the infinite primes and the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. We have $\mathcal{J}_K/\mathcal{J}_K^{S_\infty} \simeq \mathcal{D}_K$; take $\alpha = (\alpha_\mathfrak{p}) \in \mathcal{J}_K$ then $a = \prod_{\mathfrak{p}\not|\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$ is an element of $\mathcal{D}_K$, and the class of this divisor modulo $\mathcal{P}_K$ can be written $a_i \cdot \mathcal{P}_K$, so $a = a_i \cdot d$ where d is a principal divisor: $d \in \mathcal{R}_K$. Then the idele

$\alpha^{'} = \alpha \cdot d^{-1}$ is sent through the previous homomorphism to $a^{'} = \prod_{\mathfrak{p}\not|\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha^{'}_\mathfrak{p})}$ and as all primes are contained in S, we get $v_\mathfrak{p}(\alpha^{'}_\mathfrak{p}) = 0$ for all $\mathfrak{p} \notin S$. So $\alpha^{'} \in \mathcal{J}_K^S$ and consequently $\alpha \in \mathcal{J}_K^S \cdot \mathcal{R}_K$.

Step 2: the cohomology of $\mathcal{J}_L$ and $\mathcal{J}_L^S$ Introduction: If L/K is a Galois extension whose Galois group is G, we define:

$$\mathcal{J}_L^\mathfrak{p} = \textstyle\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{R}_{L_\mathfrak{P}}$$

for each prime $\mathfrak{p}$ of K.

$$\mathcal{U}_L^\mathfrak{p} = \textstyle\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{U}_{L_\mathfrak{P}}$$

As an element of G switches the primes over $\mathfrak{p}$, $\mathcal{J}_L^\mathfrak{p}$ and $\mathcal{U}_L^\mathfrak{p}$ are G-modules and so we have:

$$\mathcal{J}_L = \textstyle\prod_\mathfrak{p} \mathcal{J}_L^\mathfrak{p} \qquad \mathcal{U}_L = \prod_\mathfrak{p} \mathcal{U}_L^\mathfrak{p}$$

Given $\mathfrak{P}$ is a fixed prime of L over $\mathfrak{p}$, $G_\mathfrak{P} = \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \subseteq G$ the decomposition subgroup. If σ runs through the cosets $G/G_\mathfrak{P}$ then $\sigma(\mathfrak{P})$ runs through the different primes of L over $\mathfrak{p}$, and

$$\mathcal{J}_L^\mathfrak{p} = \textstyle\prod_{\sigma\in G/G_\mathfrak{P}} \mathcal{R}_{L_{\sigma(\mathfrak{P})}} = \prod_{\sigma\in G/G_\mathfrak{P}} \sigma(\mathcal{R}_{L_\mathfrak{P}})$$

$$\mathcal{U}_L^\mathfrak{p} = \textstyle\prod_{\sigma\in G/G_\mathfrak{P}} \mathcal{U}_{L_{\sigma(\mathfrak{P})}}$$

Recall: If g is a subgroup of finite index in G we can describe the induced G-module by $M_G^g = \bigoplus_{\sigma\in G/g} \sigma(B)$

Proposition 3.2.4. *$\mathcal{J}_L^\mathfrak{p}$ et $\mathcal{U}_L^\mathfrak{p}$ are induced G-modules and*

$$\mathcal{J}_L^\mathfrak{p} = M_G^{G_\mathfrak{P}}(\mathcal{R}_{L_\mathfrak{P}}); \mathcal{U}_L^\mathfrak{p} = M_G^{G_\mathfrak{P}}(\mathcal{U}_{L_\mathfrak{P}})$$

Convention: If S is a set of primes of K we define: $J_L^S = J_L^{\overline{S}}$, where $\overline{S}$ is the set of primes of L over S. Then we have the decomposition of G-modules:

$$\mathcal{J}_L^S = \prod_{\mathfrak{p}\in S}(\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{R}_{L_\mathfrak{P}}) \prod_{\mathfrak{p}\notin S}(\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{U}_{L_\mathfrak{P}})$$

so using our notations,

$$\mathcal{J}_L^S = \prod_{\mathfrak{p}\in S} \mathcal{J}_L^\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin S} \mathcal{U}_L^\mathfrak{p}.$$

Proposition 3.2.5. *If S is the set of primes containing the infinite primes and those which ramify, then for $i = 0, 1$ we get:*

$$i)\ H^i(G, \mathcal{J}_L^S) \simeq \bigoplus_{\mathfrak{p}\in S} H^i(G_\mathfrak{P}, \mathcal{R}_{L_\mathfrak{P}})$$

where $\mathfrak{P}$ is a prime of L over $\mathfrak{p}$, $G_\mathfrak{P}$ is the decomposition sub-group

$$ii)\ H^i(G, \mathcal{J}_L) = \bigoplus_{\mathfrak{p}} H^i(G_\mathfrak{P}, \mathcal{R}_{L_\mathfrak{P}})$$

Proof.
$$\mathcal{J}_L^S = \bigoplus_{\mathfrak{p}\in S} \mathcal{J}_L^{\mathfrak{p}} \oplus V \quad \text{where} \quad V = \prod_{\mathfrak{p}\notin S} \mathcal{U}_L^{\mathfrak{p}}.$$
We obtain for $i = 0, 1$ the isomorphism:
$$\mathrm{H}^i(G, \mathcal{J}_L) = \bigoplus_{\mathfrak{p}\in S} \mathrm{H}^i(G, \mathcal{J}_L^{\mathfrak{p}}) \oplus \mathrm{H}^i(G, V)$$
and the injection:
$$\mathrm{H}^i(G, V) \longrightarrow \prod_{\mathfrak{p}\notin S} \mathrm{H}^i(G, \mathcal{U}_L^{\mathfrak{p}}).$$
Moreover by the previous proposition $\mathcal{J}_L^{\mathfrak{p}}$ and $\mathcal{U}_L^{\mathfrak{p}}$ are induced G-modules, so
$$\mathrm{H}^i(G, \mathcal{J}_L^{\mathfrak{p}}) \simeq \mathrm{H}^i(G, M_G^{G_{\mathfrak{P}}} \mathcal{R}_{L_{\mathfrak{P}}}) \simeq \mathrm{H}^i(G_{\mathfrak{P}}, \mathcal{R}_{L_{\mathfrak{P}}})$$
$$\mathrm{H}^i(G, \mathcal{U}_L^{\mathfrak{p}}) \simeq \mathrm{H}^i(G, M_G^{G_{\mathfrak{P}}} \mathcal{U}_{L_{\mathfrak{P}}}) \simeq \mathrm{H}^i(G_{\mathfrak{P}}, \mathcal{U}_{L_{\mathfrak{P}}})$$
Recall (Neukirch p. 10-11:) if g is a sub-group of finite index in G, B a g-module then $H^i(G, M_G^g B) \simeq H^i(g, B)$ for $i = 0, 1$. Due to the choice of S, if $\mathfrak{p} \notin S$ then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an unramified ℓ-extension and $\mathrm{H}^i(G_{\mathfrak{P}}, \mathcal{U}_{L_{\mathfrak{P}}}) = 1$, using the next proposition. □

Proposition 3.2.6. *Assume $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an unramified ℓ-extension then:*
$$H^i(Gal(L_{\mathfrak{P}}/K_{\mathfrak{p}}), U_{L_{\mathfrak{P}}})) = 1 \textit{ for } i = 0, 1.$$

Proof. The following exact sequence:
$$1 \longrightarrow \mathcal{U}_{L_{\mathfrak{P}}} \longrightarrow \mathcal{R}_{L_{\mathfrak{P}}} \longrightarrow \mathbb{Z}_\ell \longrightarrow 1$$
induces a long sequence of cohomology:
$$1 \longrightarrow \mathcal{U}_{K_{\mathfrak{p}}} \longrightarrow \mathcal{R}_{K_{\mathfrak{p}}} \longrightarrow \mathbb{Z}_\ell \twoheadrightarrow \mathrm{H}^1(\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}), \mathcal{U}_{L_{\mathfrak{p}}})$$
where the map $\mathcal{R}_{K_{\mathfrak{p}}} \longrightarrow \mathbb{Z}_\ell$ is the restriction of the valuation $v_{L_{\mathfrak{P}}}$. As $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an unramified extension: $e_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = 1$; this restriction is surjective:
$$\mathrm{H}^1(\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}), \mathcal{U}_{L_{\mathfrak{P}}})) = 1$$
and using the local class field axiom, the Herbrand quotient is trivial:
$$h(\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}), \mathcal{U}_{L_{\mathfrak{P}}})) = 1$$
so we deduce:
$$\mathrm{H}^0(\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}), \mathcal{U}_{L_{\mathfrak{P}}})) = 1.$$
□

Let's go back to the proof: Consequently we obtain
$$\mathrm{H}^i(G, \mathcal{J}_L^S) \simeq \bigoplus\nolimits_{\mathfrak{p}\in S} \mathrm{H}^i(G_{\mathfrak{P}}, \mathcal{R}_{L_{\mathfrak{P}}})$$

And using the second part,

$$\mathrm{H}^i(G,\mathcal{J}_L) = \varprojlim_S \mathrm{H}^i(G,\mathcal{J}_L^S) = \varprojlim_S \bigoplus_{\mathfrak{p}} \mathrm{H}^i(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}}) = \bigoplus_{\mathfrak{p}} \mathrm{H}^i(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}})$$

Step 3: The ℓ-group of S-units is defined by: $\mathcal{E}_K^S = \mathcal{R}_K \cap \mathcal{J}_K^S$ We have to show that if S is a set of primes containing the infinite primes and the primes which ramify in L then:

$$h(G,\mathcal{E}_L^S) = \tfrac{1}{\ell^n}\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$$

where $n_{\mathfrak{p}}$ denotes the index of the decomposition sub-group. This is due to the fact that the Herbrand quotient linked to a Galois module in a cyclic extension only depends to the character of the representation which is associated: indeed it gives the structure of G-module up to a finite; and we use the property which says that if you consider a sub-module of finite index then its Herbrand quotient is trivial; and this character is given by the Herbrand's representation character.

Step 4: conclusion Assume S is the set of primes described before, then we have the following exact sequence:

$$1 \longrightarrow \mathcal{E}_L^S \longrightarrow \mathcal{J}_L^S \longrightarrow \mathcal{J}_L^S \cdot \mathcal{R}_L/\mathcal{R}_L = \mathcal{C}_L \longrightarrow 1.$$

As L/K is a cyclic ℓ-extension, by the property of the Herbrand quotient, we get:

$$h(G,\mathcal{J}_L^S) = h(G,\mathcal{E}_K^S)\cdot h(G,\mathcal{C}_L)$$

But

$$\mathrm{H}^i(G,\mathcal{J}_L^S) \simeq \prod_{\mathfrak{p}\in S} \mathrm{H}^i(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}})$$

for $i = 0, 1$, and using the local class field axiom we get:

$$|\mathrm{H}^0(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}})| = n_{\mathfrak{p}}$$

$$|\mathrm{H}^1(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}})| = 1$$

So,

$$h(G,\mathcal{J}_L^S) = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$$

And by step 3: $h(G,\mathcal{E}_L^S) = \frac{1}{\ell^n}\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$, we deduce:

$$h(G,\mathcal{C}_L) = \ell^n$$

Theorem 3.2.2. *If L/K is a cyclic ℓ-extension of algebraic number fields then:*

$$|H^i(G(L/K),\mathcal{C}_L)| = \begin{cases} [L:K] & \text{for } i=0 \\ 1 & \text{for } i=1 \end{cases}$$

Proof. By the Herbrand quotient of the idele class ℓ-group one gets;

$$h(G(L/K), \mathcal{C}_L) = [L : K] = \ell^n$$

as by hypothesis L/K is a cyclic ℓ-extension. It therefore suffices to show that

$$\mathrm{H}^{-1}(G(L/K), \mathcal{C}_L) = \mathrm{H}^1(G(L/K), \mathcal{C}_L) = 1$$

as G is a cyclic group.

We prove this by induction on the degree n.

(i) If $n = 0$ then $L = K$ so this is true.

(ii) Assume $n \geq 1$ and that the property is true for the rank $n-1$, let's consider L/K an extension of degree ℓ^n.

1) If $n > 1$ then $\ell < \ell^n$, let M/K be a sub-extension of L/K of prime degree ℓ.

$$\begin{array}{c} L \\ | \\ M \\ | \\ K \end{array}$$

Recall: If g is a normal subgroup of G, let A be a G-module, then we have the following exact sequence:

$$0 \longrightarrow \mathrm{H}^1(G/g, A^g) \longrightarrow \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(g, A)$$

so we obtain the following exact sequence:

$$1 \longrightarrow \mathrm{H}^1(G(M/K), \mathcal{C}_M) \longrightarrow \mathrm{H}^1(G(L/K), \mathcal{C}_L) \longrightarrow \mathrm{H}^1(G(L/M), \mathcal{C}_L)$$

and by assumption

$$\mathrm{H}^1(G(M/K), \mathcal{C}_M) = 1 \text{ as } |G(M/K)| = \ell$$

$$\mathrm{H}^1(G(L/M), \mathcal{C}_L) = 1 \text{ car } |G(L/M)| = \ell^{n-1} < \ell^n$$

Consequently using the previous exact sequence, we get

$$\mathrm{H}^1(G(L/K), \mathcal{C}_L) = 1$$

2) If $n = 1$ then L/K is a cyclic extension of prime degree ℓ

We have this exact sequence:

$$1 \longrightarrow \mathcal{R}_L \longrightarrow \mathcal{J}_L \longrightarrow \mathcal{C}_L$$

By the Herbrand quotient (as G is cyclic) one gets:

$$\begin{tikzcd}
 & \mathrm{H}^0(G,\mathcal{R}_L) \arrow[r] & \mathrm{H}^0(G,\mathcal{J}_L) \arrow[dr] & \\
\mathrm{H}^{-1}(G,\mathcal{C}_L) \arrow[ur] & & & \mathrm{H}^0(G,\mathcal{C}_L) \arrow[dl] \\
 & \mathrm{H}^{-1}(G,\mathcal{J}_L) \arrow[ul] & \mathrm{H}^{-1}(G,\mathcal{R}_L) \arrow[l] &
\end{tikzcd}$$

And by the cohomology of the group of ideles $\mathcal{J}_L$ one gets:

$$\mathrm{H}^i(G,\mathcal{J}_L^S) \simeq \prod_{\mathfrak{p}\in S} \mathrm{H}^i(G_{\mathfrak{P}},\mathcal{R}_{L_{\mathfrak{P}}}).$$

By the local class field axiom, one deduces $\mathrm{H}^1(G,\mathcal{J}_L)=1$. As we know the Herbrand quotient of the idele class ℓ-group we just have to show that for L/K a cyclic extension of prime degree $\mathrm{H}^{-1}(G,\mathcal{C}_L)=1$. So it suffices to prove that the map from $\mathrm{H}^0(G,\mathcal{R}_L)$ to $\mathrm{H}^0(G,\mathcal{J}_L)$ is injective, which is true to the next ℓ-adic Hasse Norm Theorem. Consequently for L/K a cyclic extension of prime degree ℓ one gets :

$$\mathrm{H}^1(\mathrm{Gal}(L/K),\mathcal{C}_L)=1$$

□

Theorem 3.2.3. ***The ℓ-adic Hasse Norm Theorem*** *If L/K is a cyclic extension of prime degree ℓ, an element of the ℓ-group of principal ideles is a norm from L/K if and only if it is a norm everywhere locally, i.e a norm from the completion $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ where $\mathfrak{P}|\mathfrak{p}$.*

Proof. Let x be a principal idele such that $x=N_{L/K}(y)$ where $y\in\mathcal{R}_L$. Since $\mathcal{R}_L$ can be injected in $\mathcal{J}_L$, which can be surjected in $\mathcal{R}_{L_{\mathfrak{P}}}$ taking the $\mathfrak{p}$-components one can deduce that x is a norm everywhere locally.

Conversely assume $x\in\mathcal{R}_K$ and write down $x=\bar{x}.y^\ell$ as $K^\times/{K^\times}^\ell \simeq \mathcal{R}_K/\mathcal{R}_K^\ell$, where $\bar{x}$ denotes the image of x modulo ${K^\times}^\ell$. Since L/K is a cyclic ℓ-extension, y^ℓ is a norm. Moreover, by hypothesis x is a norm everywhere locally which means that each component $\bar{x}_{\mathfrak{p}}$, for all $\mathfrak{p}$, is a norm. Using the usual Hasse norm theorem one can deduce that x is a norm. □

3.3 The degree

We fix an isomorphism such that :

$$\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \simeq \mathbb{Z}_\ell.$$

Then the degree map is defined by restriction as following :

$$\begin{array}{rcccc}
\deg & : & G=\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) & \to & \mathbb{Z}_\ell \\
 & & \phi & \mapsto & \phi_{|\tilde{\mathbb{Q}}}
\end{array}$$

where $\mathbb{Q}^{ab}$ is the maximal abelian la pro-ℓ-extension of $\mathbb{Q}$

$$\begin{array}{c} \mathbb{Q}^{ab} \\ | \\ \tilde{\mathbb{Q}} \\ | \\ \mathbb{Q} \end{array}$$

If $K/\mathbb{Q}$ is a finite extension, we define: $f_K = [K \cap \tilde{\mathbb{Q}} : \mathbb{Q}]$ and we obtain by analogy with the local case a surjective homomorphism

$$d_K = \frac{1}{f_K} \cdot d : \; G_K \longrightarrow \mathbb{Z}_\ell$$

$$\begin{array}{ccc} K & \text{——} & \widetilde{K} \\ | & & | \\ \mathbb{Q} & \text{——} & \widetilde{\mathbb{Q}} \end{array}$$

where $\tilde{K} = K\widetilde{\mathbb{Q}}$.

3.4 The G-module

For the $G_{\mathbb{Q}}$-module A we consider the union of the idele class ℓ-group $\mathcal{C}_K$ where K runs through the finite extensions of K:

$$A = \bigcup_{[K:\mathbb{Q}]<\infty} \mathcal{C}_K.$$

So $A_K = \mathcal{C}_K$. For a finite and abelian ℓ-extension, we define the following isomorphism:

$$[\;,\;, L/K] = \textstyle\prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \text{ for } \alpha \in \mathcal{J}_K$$

where $L_{\mathfrak{p}}$ denotes the completion of $K_{\mathfrak{p}}$ for a prime $\mathfrak{P}|\mathfrak{p}$ and $(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$ denotes the local symbol. By the local class field theorem for all finite and abelian ℓ-extension of a local field, one gets:

$$\mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \simeq \mathcal{R}_{K_{\mathfrak{p}}}/N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\mathcal{R}_{L_{\mathfrak{P}}}$$

Proposition 3.4.1. *If L/K and L'/K' are finite and abelian ℓ-extensions of number fields such that $K \subseteq K'$ and $L \subseteq L'$, then the following diagram is commutative:*

$$\begin{array}{ccc} \mathcal{J}_{K'} & \xrightarrow{[\,\cdot\,, L'/K']} & \mathrm{Gal}(L'/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow \\ \mathcal{J}_K & \xrightarrow{[\,\cdot\,, L/K]} & \mathrm{Gal}(L/K) \end{array}$$

Proof. Take $\alpha = (\alpha_{\mathfrak{P}}) \in \mathcal{J}_{K'}$. On the one hand, one gets:

$$(\alpha_{\mathfrak{P}}, L^{'}_{\mathfrak{P}}/K^{'}_{\mathfrak{P}})_{/L_{\mathfrak{p}}} = (N_{K^{'}_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}), L_{\mathfrak{p}}/K_{\mathfrak{p}}) \text{ pour } \mathfrak{P}|\mathfrak{p}$$

And one the other hand:

$$[N_{K'/K}(\alpha), L/K] = \prod_{\mathfrak{p}}(N_{K'/K}(\alpha)_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}}(N_{K'_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}) = \prod_{\mathfrak{P}}(\alpha_{\mathfrak{P}},, L'_{\mathfrak{P}}/K'_{\mathfrak{P}})_{/L} = [\alpha, L'/K']_{/L}.$$

Remark: Neukirch p. 90 The previous proposition is still true if L/K is an infinite and abelian ℓ-extension with $[\alpha, L/K] = \prod_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$ where $L_{\mathfrak{p}}$ denotes the union of the completions $L'_{\mathfrak{p}}/K_{\mathfrak{p}}$ for all finite sub-extensions. The goal is to show that

$$\forall a \in \mathcal{R}_K,\ [a, \tilde{K}/K] = 1.$$

$\tilde{K}/K$ is contained in the extension of K obtained by adjoining roots of units. If we show that $[a, (K(\zeta)/K)_\ell] = 1$, for a an element of the ℓ-group of principal ideles and for ζ a root of unit one could deduce that $[a, \tilde{K}/K] = 1$ for $\forall a \in \mathcal{R}_K$, where $(K(\zeta)/K)_\ell$ denotes the projection on the ℓ- Sylow sub-group of $\mathrm{Gal}(K(\zeta)/K)$ (in order to use the ℓ-adic local symbol it is necessary to work with an ℓ-extension, this explains the use of the projection). So the homomorphism $[\ \cdot\ , \tilde{K}/K]/\mathcal{J}_K \longrightarrow G(\tilde{K}/K)$ induces a new homomorphism, still denoted $[\ \cdot\ , \tilde{K}/K]$ such that $[\ \cdot\ , \tilde{K}/K]/\mathcal{C}_K \longrightarrow G(\tilde{K}/K)$ as $\mathcal{R}_K \subseteq \mathrm{Ker}([, \tilde{K}/K])$. □

Proposition 3.4.2. *For all roots of units ζ and for all $a \in \mathcal{R}_K$ one gets*

$$[a, (K(\zeta)/K)_\ell] = 1.$$

Proof. We use the previous proposition $[N_{K/\mathbb{Q}}(a), (\mathbb{Q}(\zeta)/\mathbb{Q})_\ell] = [a, (K(\zeta)/K)_\ell]_{/\mathbb{Q}(\zeta)}$. Consequently it suffices to show the property for $K = \mathbb{Q}$. But

$$[a, (\mathbb{Q}(\zeta)/\mathbb{Q})_\ell]\zeta = \prod_{\mathfrak{p}}(a, (\mathbb{Q}_p(\zeta)/\mathbb{Q}_p))_\ell.$$

Let's consider ζ a q^m root of units, with $q^m \neq 2$. We take $a \in \mathcal{R}_{\mathbb{Q}_p}$ and write $a = u_p \cdot p^{v_p(a)}$ where v_p is the usual normalized valuation on $\mathbb{Q}_p$, which takes values in $\mathbb{Z}_\ell$. For $p \neq q$ and $p \neq \infty$ the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is an unramified extension. Due to the fundamental principle given by Neukirch (p. 30 Class Field Theory) which says that the local symbol associates the uniformising element to the Frobenius, one gets that $(p, (\mathbb{Q}_p(\zeta)/\mathbb{Q}_p))_\ell$ corresponds to the Frobenius automorphism $\phi_p : \zeta \longrightarrow \zeta^p$. Moreover the following diagram is a commutative one:

$$\begin{tikzcd}
K_{\mathfrak{p}}^{\times} \arrow[r, "(\ \cdot\ ;\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}))"] \arrow[d] & \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \arrow[d] \\
\mathcal{R}_{K_{\mathfrak{p}}} \arrow[r, "(\ \cdot\ ;\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}))_\ell"] & \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})_\ell
\end{tikzcd}$$

the symbol on the top is the usual local symbol, and the symbol on the bottom is the ℓ-adic local symbol. Consequently, one deduces

$$(a, (\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)_\ell) = \zeta^{n_p}$$

with

$$n_p = \begin{cases} p^{v_p(a)} & \text{for } p \neq q \text{ et } p \neq \infty \\ u_p^{-1} & \text{for } p = q \\ sgn(a) & \text{for } p \neq \infty \end{cases}$$

So

$$[a, (\mathbb{Q}(\zeta)/\mathbb{Q})_\ell]\zeta = \prod_{\mathfrak{p}}(a, (\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)_\ell) = \zeta^\alpha$$

And due to the product formula, $\alpha = \prod_p n_p = sgn(a) \cdot \prod_{p\neq\infty} p^{v_p(a)} \cdot a^{-1} = 1.$ □

3.5 The valuation

Definition: We consider the valuation $v_K : \mathcal{C}_K \longrightarrow \mathbb{Z}_\ell$ defined as following:

$$\mathcal{C}_K \overset{[\,\cdot\,,\tilde{K}/K]}{\longrightarrow} G(\tilde{K}/K) \xrightarrow{d_K} \mathbb{Z}_\ell$$

Proposition 3.5.1. *This application, well-defined, $v_K : \mathcal{C}_K \longrightarrow \mathbb{Z}_\ell$ is surjective and is henselian with respect to the degree.*

Proof. 1)For the surjectivity

(i) Let's prove first that if L/K is a finite sub-extension of $\tilde{K}/K$ then the map $[\,\cdot\,, L/K] : \mathcal{J}_K \longrightarrow G(L/K)$ defined before by

$$[\alpha, L/K] = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \quad \text{for} \quad \alpha \in \mathcal{J}_K$$

is surjective. Indeed the local symbol is surjective: so if one takes an element of the decomposition subgroup one gets a preimage in $\mathcal{R}_{K_{\mathfrak{p}}}$ and so in $\mathcal{J}_K$. So the image of the ℓ-group of ideles through this morphism, denoted by $[\mathcal{J}_K, \mathrm{Gal}(L/K)]$, contains all decomposition subgroups $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, for all $\mathfrak{p}$ which decomposes completely in the field M, the field of fixed points of $[\mathcal{J}_K, \mathrm{Gal}(L/K)]$. So one deduces $M = K$ and $[\mathcal{J}_K, \mathrm{Gal}(L/K)] = \mathrm{Gal}(L/K)$ and that $[\mathcal{J}_K, \mathrm{Gal}(\tilde{K}/K)]$ is dense in $\mathrm{Gal}(\tilde{K}/K)$.

(ii) Moreover one gets $[\mathcal{J}_K, \mathrm{Gal}(\tilde{K}/K) = [\mathcal{C}_K, \mathrm{Gal}(\tilde{K}/K)]$ due to the property of the ℓ-group of ideles. The goal is to show that this subgroup is both closed and dense in $[\mathcal{C}_K, \mathrm{Gal}(\tilde{K}/K)]$, so one can deduce that

$$[\mathcal{C}_K, \mathrm{Gal}(\tilde{K}/K)] = \mathrm{Gal}(\tilde{K}/K)$$

Consequently $v_K = d_K \circ [\,\cdot\,, \mathrm{Gal}(\tilde{K}/K)]$ is surjective as the composition of two surjections.

The previous step shows that $[\mathcal{J}_K, \mathrm{Gal}(\tilde{K}/K)]$ is dense in $\mathrm{Gal}(\tilde{K}/K)$; in order to show that this image is closed in $\mathrm{Gal}(\tilde{K}/K)$ we are going to use the fact that $\mathcal{C}_{\mathcal{K}}$ est compact, and that the map $[\,\cdot\,, \mathrm{Gal}(\tilde{K}/K)]$ of $\mathcal{J}_K$ in $\mathrm{Gal}(\tilde{K}/K)$ is continuous. As it is a group homomorphism, it suffices to show that the map is continuous in the neighborhood of the neutral. Let's consider such a neighborhood in $\mathrm{Gal}(\tilde{K}/K)$ whose image is therefore of the shape of $\mathrm{Gal}(\tilde{K}/L)$, where L is a finite extension of K. The aim is to built a neighborhood of the neutral in $\mathcal{J}_K$ whose image through the map is trivial on $\mathrm{Gal}(L/K)$. Yet the idele class ℓ-group can be written as:

$$\mathcal{J}_K = \mathcal{U}_K \times \oplus \pi_{\mathfrak{p}}^{\mathbb{Z}_\ell}$$

where $\mathcal{U}_K$ is the ℓ-group of units; thus a neutral neighborhoods system is:

$$\mathcal{U}_K^{'} \times \oplus \pi_{\mathfrak{p}}^{\ell^{k_{\mathfrak{p}}}\mathbb{Z}_\ell}$$

where $\mathcal{U}_K^{'}$ is an open submodule of $\mathcal{U}_K$. We are able to choose $k_{\mathfrak{p}}$ such that the image of $\pi_{\mathfrak{p}}^{\ell^{k_{\mathfrak{p}}}\mathbb{Z}_\ell}$ is trivial through the local symbol. Indeed as $\tilde{K}/K$ is a pro-cyclic extension and L/K is a finite extension whose order is given: $[L : K] = \ell^n$, it suffices to choose for instance $k_{\mathfrak{p}} > n$. Consequently their images through the previous homomorphism are trivial on $\mathrm{Gal}(L/K)$. Moreover if $\mathfrak{p}|\ell$ then the local extension is unramified and the image of an element of $\mathcal{U}_K^{'}$ is trivial. If $\mathfrak{p} \not|\ell$ then thanks to the filtration of the group of units one can obtain a trivial image. Therefore for all neighborhood of the neutral of $\mathrm{Gal}(\tilde{K}/k)$, of the shape $\mathrm{Gal}(\tilde{K}/L)$, where L runs trough the finite and Galois extensions of K, we get a neighborhood of the neutral whose image is sent in the initial

neighborhood. Consequently the map is continuous from $\mathcal{J}_K$ with the topology of the inverse limit, in $\mathrm{Gal}(\tilde{K}/K)$ with the Krull's topology. That is why $[\mathcal{C}_K, \mathrm{Gal}(\tilde{K}/K)]$ is closed in $\mathrm{Gal}(\tilde{K}/K)$. This image is both closed and dense, so:

$$[\mathcal{C}_K, \mathrm{Gal}(\tilde{K}/K)] = \mathrm{Gal}(\tilde{K}/K).$$

2) For the second point (ii) of the definition of a henselian valuation one gets

$$v_K(N_{L/K}\mathcal{C}_L) = v_K(N_{L/K}\mathcal{J}_L) = d_K \circ [N_{L/K}\mathcal{J}_L, \tilde{K}/K]$$

using the definition of the valuation and the fact that a principal idele has a trivial image through the following map $[\,\cdot\,, \mathrm{Gal}(\tilde{K}/K)] : [\mathcal{R}_K,\ \mathrm{Gal}(\tilde{K}/K)] = 1$. Moreover $d_K = \frac{1}{f_K} \cdot d$ and $f_{L/K} = f_L/f_K$ so that $d_K = f_{L/K} \cdot d_L$. Due to the previous proposition, the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{J}_{L'} & \xrightarrow{[\,\cdot\,\tilde{L}/L]} & \mathrm{Gal}(\tilde{L}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow \\ \mathcal{J}_K & \xrightarrow{[\,\cdot\,\tilde{K}/K]} & \mathrm{Gal}(\tilde{K}/K) \end{array}$$

consequently one gets $[N_{L/K}\mathcal{J}_L, \tilde{K}/K] = [\mathcal{J}_L, \tilde{L}/L]$ so one deduces:

$$v_K(N_{L/K}\mathcal{C}_L) = f_{L/K} d_L \circ [\mathcal{J}_L, \tilde{L}/L] = f_{L/K} v_L(\mathcal{C}_L) = f_{L/K}\mathbb{Z}_\ell$$

using the fact that v_L is surjective. $\square$

3.6 Conclusion

Theorem 3.6.1. *Let L be a Galois ℓ-extension of a number field K, let (deg, v) be a class field theory and let $A_K = \mathcal{C}_K$ be a Gal(L/K)-module satisfying the class field axiom then one gets the following isomorphism:*

$$Gal(L/K)^{ab} \simeq \mathcal{C}_K/N_{L/K}\mathcal{C}_L.$$

In particular for all abelian ℓ-extensions of a number field, one gets:

$$Gal(L/K) \simeq \mathcal{C}_K/N_{L/K}\mathcal{C}_L.$$

We therefore obtain a one to one correspondence between finite and abelian ℓ-extensions of a number field K and open subgroups of $\mathcal{C}_K$.

4 Conclusion

Neukirch's abstract theory allows to prove the existence of the reciprocity map in the context of ℓ-adic class field theory. Applying this abstract theory in the logarithmic context [Ja2], we hope to obtain new results, the more so as the logarithmic valuation is henselian.

References

[AT] E. Artin & J. Tate, *Class field theory*, Benjamin, New York, 1967

[Ja1] J.-F. Jaulent, *Théorie ℓ-adique du corps des classes*, J. Théor. Nombres Bordeaux, **10**, fasc.2 (1998), 355–397.

[Ja2] J.-F Jaulent, *Sur l'indépendance ℓ-adique de nombres algébriques*, J. Théor. Nombres Bordeaux, **20**, fasc.2 (1985)

[Ja3] J.-F Jaulent, *Classes logarithmiques d'un corps de nombres*, J. Théor. Nombres Bordeaux, **6**, (1994), 301–325.

[La] S. Lang, *Cyclotomic Fields*, Springer Verlag, GTM 59, (1978)

[Li] Q. Liu, *Algebraic geometry and algebraic curves*, Oxford University Press, GTM 6, (2006)

[Ne] J. Neurkirch, *Class Field Theory*, Springer-Verlag, GTM 280, (1986)

[Ne] J. Neurkirch, *Algebraic Number Theory*, Springer-Verlag, GTM 322, (1986)

[Wa] L. Washington, *An introduction to Cyclotomic fields*, Springer Verlag, GTM 83, (1997)

Acknowledgements

I would like to thank Boas Erez for proposing me this question and my advisor Jean-François Jaulent for his helpful comments on earlier versions of this article.

Adresses

Univ. Bordeaux, Institut de Mathématiques de Bordeaux, UMR 5251, 351 Cours de la Libération, F-33405 Talence cedex

CNRS, Institut de Mathématiques de Bordeaux, UMR 5251, 351 Cours de la Libération, F-33405 Talence cedex

Courriel

`stephanie.reglade@math.u-bordeaux1.fr`